Exploit:Win32/Pdfjsc.YP

Article URL
malware.php?mal_id=2953612075eab865f9ebd28.10607119

Author
SecurityHome.eu

Published: 01 May 2020

Aliases :

Exploit:Win32/Pdfjsc.YP

is also known as *Exploit.JS.Pdfka.fhr, Exploit.PDF-JS.BN, Exploit.PDF.2645, JS/Exploit.Pdfka.PFU trojan, PDF.Exploit, Exploit.JS.Pdfka.fhr, Troj/PDFEx-ET*

.

Explanation :

Exploit:Win32/Pdfjsc.YP is a specially-crafted Portable Document Format (PDF) file that exploits a vulnerability in Adobe Acrobat and Adobe Reader described in the following articles:

CVE-2010-0188 APSB10-07

Exploit:Win32/Pdfjsc.YP is known to be part of the "Blackhole" malware distribution kit.

The PDF file contains malicious JavaScript that checks if it is run on a computer with a vulnerable version of Adobe Acrobat or Adobe Reader. If this is true, Exploit:Win32/Pdfjsc.YP connects to a remote server to download a file, which may be malicious.

Some of the servers it is known to connect to are:

stopeatingmyglasses.com crdret.ru

The file is then saved in the computer as "wpbt0.dll".

As of this writing, the files are no longer available.

Analysis by Daniel Chipiristeanu

Last update 01 May 2020